

21. A distributed digital rights system including:

a user located at a first site, the first site including a first secure environment;

a rightsholder located at a second site, the second site including a second secure environment;

a first clearinghouse node located at a third site, the third site including a third secure environment and including an apparatus allowing the first clearinghouse node to assume a plurality of roles in clearing a transaction;

a second clearinghouse node located at a fourth site, the fourth site including a fourth secure environment and including an apparatus allowing the second clearinghouse node to assume a plurality of roles in clearing a transaction; and

a distributed digital apparatus allowing the first clearinghouse node and the second clearinghouse node to participate cooperatively in clearing a first transaction and in clearing a second transaction, wherein the first clearinghouse plays a first role in clearing the first transaction, the second clearinghouse plays a second role in clearing the first transaction, the first clearinghouse plays the second role in clearing the second transaction, and the second clearinghouse plays the first role in clearing the second transaction.

22. A distributed digital rights system as in Claim 21, in which the distributed digital apparatus includes hardware and software elements.

B1

23. A distributed digital rights system as in Claim 21, in which the first role consists of a first step in financially clearing a transaction, and the second role consists of a second step in financially clearing a transaction.

24. A distributed digital rights system as in Claim 21, in which the first role consists of financially clearing a transaction, at least in part, and the second role consists of analyzing and reporting usage information relating to a transaction.

25. A method for performing clearing functions including:

- initiating a first secure transaction involving a user and a rights holder, resulting in the user agreeing to provide consideration for access to or other use of protected content;
- securely communicating with a first clearinghouse node located at a first site, the communication including information relating to the first transaction;
- securely communicating with a second clearinghouse node located at a second site, the communication including information relating to the first transaction;
- the first and second clearinghouse nodes operating to at least partially clear the first transaction, including the first clearinghouse node undertaking a first step in the clearing and the second clearinghouse node undertaking a second step in the clearing;
- initiating a second transaction involving a user and a rights holder, resulting in the user agreeing to provide consideration for access to or other use of protected content;

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT
& DUNNER, L.L.P.
STANFORD RESEARCH PARK
700 HANSEN WAY
PALO ALTO, CALIF. 94304
650-849-6600

securely communicating with the first clearinghouse node, the communication including information relating to the second transaction;

securely communicating with the second clearinghouse node, the communication including information relating to the second transaction;

the first and second clearinghouse nodes operating to at least partially clear the second transaction, the first clearinghouse node undertaking the second step in the clearing and the second clearinghouse node undertaking the first step in the clearing.

26. A method as in Claim 25, in which the first step includes obtaining access to information relating to the identity of the user, eliminating or altering at least a portion of the identity information, and passing information relating to the transaction to the clearinghouse node which performs the second step, whereby the node which performs the second step is not able to ascertain the identity of the user.

27. A method as in Claim 25, in which:

the first transaction information communicated to the first and second clearinghouse nodes includes a first rule; and

the second transaction information communicated to the first and second clearinghouse nodes includes a second rule.

28. A method as in Claim 27, in which:
the roles played by the first and second clearinghouse nodes in clearing the first transaction are at least in part dictated by the first rule; and
the roles played by the first and second clearinghouse nodes in clearing the second transaction are at least in part dictated by the second rule.

29. A method as in Claim 28, in which:
the first clearing step includes aggregating information from at least two transactions; and
the second clearing step includes communicating payment-related information to a rightsholder.

30. A method of at least partially clearing a digital transaction, including performing the following steps at a clearinghouse node:
receiving a first rule set associated with a first party,
receiving a second rule set associated with a second party;
receiving information relating to a transaction between a user and a rightsholder;
and
at least partially clearing the transaction, using a rule from the first rule set and a rule from the second rule set to at least in part control the clearing process.

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT
& DUNNER, L.L.P.
STANFORD RESEARCH PARK
700 HANSEN WAY
PALO ALTO, CALIF. 94304
650-849-8600

B

31. A method as in Claim 30, in which:
the first party is the user; and
the second party is the rightsholder.

32. A method as in Claim 31, in which:
the first rule set at least in part governs the use of information relating to the identity of the user.

33. A method as in Claim 30, further including:
transmitting information relating to the transaction to a third party, the transmission being governed, at least in part, by the first rule set and the second rule set.

34. A method as in Claim 32, further including:
the third party aggregating at least a portion of the transmitted information with other information and transmitting the aggregated information to the rightsholder, the aggregation and transmission being governed, at least in part, by the second rule set.

35. A method as in Claim 30, further including:
generating a third rule set, the generation process being governed, at least in part, by the first rule set and the second rule set; and
communicating information relating to the transaction to a third party, the communication being governed, at least in part, by the third rule set.

36 A method of performing a digital transaction, including the following steps:
a user located at a first location initiating a secure communication with a clearinghouse node located at a second location, the secure communication including a request for use of a governed digital object;
the clearinghouse node checking to determine whether a rightsholder has granted the user a right to use the governed digital object and determining that no such right has been granted;
the clearinghouse node informing the user that the user lacks the right to use the governed digital object;
the user making a request to the clearinghouse node to obtain the right necessary to use the governed digital object;
the clearinghouse node checking to determine whether the rightsholder has authorized the clearinghouse to grant such rights, and, if so, upon what terms;
the clearinghouse determining that the rightsholder has authorized the clearinghouse node to grant the rights necessary to use the governed digital object, if the user agrees to terms acceptable to the rightsholder;
the clearinghouse node and the user engaging in a secure digital negotiation, in which the clearinghouse node proposes terms to the user, the user rejects at least one term, and proposes terms which differ in at least one respect from those proposed by the clearinghouse node, and the clearinghouse node determines that the user's proposed terms are consistent with the terms required by the rightsholder;

B
LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT
& DUNNER, L.L.P.
STANFORD RESEARCH PARK
700 HANSEN WAY
PALO ALTO, CALIF. 94304
650-849-6600

the clearinghouse node securely communicating the results of the negotiation to the user;

in response to the communication from the clearinghouse node, the user providing agreed-upon compensation; and

the clearinghouse node providing the user with access to the governed digital object. |

37. A method as in Claim 36, in which the step of the clearinghouse node checking to determine whether the rightsholder has authorized the clearinghouse to grant such rights includes the clearinghouse node checking local storage to determine if such authorization has been granted, and does not include any direct communication with the rightsholder.

38. A method as in Claim 36, in which:

the governed digital object is communicated to the first location prior to the user communicating the request for use of the governed digital object; and

the step of the clearinghouse node providing the user with access to the governed digital object includes the clearinghouse providing a rule to the user.

B

39. A method as in Claim 36, further including:
the user making a use of at least a portion of the governed digital object; and
information relating to the user's use being communicated to the clearinghouse, the
communication being consistent with the results of the negotiation.

40. A method as in Claim 36, in which the term rejected by the user relates to
collection or use of information concerning the user's identity.

41. A method of clearing a digital transaction, including the following steps:
specifying a first specialized clearinghouse for clearing transactions relating to a first
vertical market and a second specialized clearinghouse for clearing transactions
relating to a second vertical market;
commencing the digital transaction;
communicating information relating to the transaction to a first general
clearinghouse node;
the first general clearinghouse node analyzing the information and determining that
the digital transaction falls within the first vertical market or the second vertical market;
based on the results of the determination, the first general clearinghouse node
selecting between the first specialized clearinghouse and the second specialized
clearinghouse;
the first general clearinghouse node securely communicating with the selected
specialized clearinghouse; and

the selected specialized clearinghouse taking part in clearing the digital transaction.

42. A method as in Claim 41, in which the first vertical market relates to distribution of digital music and the second vertical market relates to distribution of digital video.

43. A method as in Claim 41, in which the digital transaction relates to use of digital content by an end user, and the first general clearinghouse node is selected, at least in part, by the end-user.

44. A method as in Claim 41, in which the digital transaction relates to use of digital content by an end user; further including:

the end user receiving a secure digital container containing the digital content, the digital content being governed by a rule set, and

the first general clearinghouse node is chosen, at least in part, as a result of requirements imposed by the rule set.

45. A method as in Claim 44, in which the rule set includes a rule specified by the first general clearinghouse node.

B1

46. A method as in Claim 41, in which the first vertical market relates to distribution of a first class of digital music and the second vertical market relates to distribution of a second class of digital music.

47. A method of clearing a digital transaction including:
initiating a secure digital transaction involving a user and a rightsholder;
in connection with the digital transaction, the user agreeing to provide consideration, the consideration to be cleared through a clearinghouse;
the user selecting a payment method;
the user selecting a clearinghouse from at least two clearinghouses available for clearing the transaction;
the user securely communicating information relating to the transaction to the selected clearinghouse; and
the selected clearinghouse participating in the clearing of the transaction.

48. A method as in Claim 47, in which the secure digital transaction involves the use of governed digital content; and further including:
the user receiving the governed digital content in a secure container, the secure container having associated a rule set made up of at least one rule; and
the steps of the user selecting a payment method, the user selecting a clearinghouse, and the user securely communicating information are all governed, at least in part, by the rule set.

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT
& DUNNER, L.L.P.
STANFORD RESEARCH PARK
700 HANSEN WAY
PALO ALTO, CALIF. 94304
650-849-6600

B

49. A method as in Claim 48, in which the rule set contains a rule from the rightsholder and a rule from the selected clearinghouse.
50. A method as in Claim 49, in which the rule set also contains a rule from a non-selected clearinghouse.
51. A method as in Claim 47, in which the information communicated from the user to the selected clearinghouse is communicated in a secure container, the secure container being governed, at least in part, by a rule set.
52. An electronic transaction method including:
 - at a user site, receiving a first digital container including protected content, the first digital container having associated a first rule set made up of one or more rules;
 - the user indicating an interest in accessing or otherwise using at least a portion of the protected content;
 - the user's indication of interest causing invocation of the first rule set, the first rule set specifying at least:
 - one or more financial clearinghouses for the clearing of consideration required for access to or other use of the content, and
 - one or more information clearinghouses for the clearing of information related to access to or other use of the content;

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT
& DUNNER, L.L.P.
STANFORD RESEARCH PARK
700 HANSEN WAY
PALO ALTO, CALIF. 94304
650-849-6600

the user selecting a financial clearinghouse from among at least two financial clearinghouses specified by the first rule set;

the user selecting an information clearinghouse from at least two information clearinghouses specified by the first rule set;

the user being provided access to at least a portion of the protected content;

financial information being securely provided to the selected financial clearinghouse;

and

other information relating to the transaction being securely provided to the selected information clearinghouse.

53. A method as in Claim 52, in which the selected financial clearinghouse and the selected information clearinghouse are the same institution.

54. A method as in Claim 52, in which the first rule set contains a rule specified by the rightsholder, and a rule specified by a clearinghouse.

55. A method as in Claim 54, further including:

incorporating the financial information in a second secure container prior to the step of securely providing the financial information to the selected financial clearinghouse, the secure container having associated a second rule set.

56. A method as in Claim 55, further including:

generating the second rule set, the generation being governed, at least in part, by the first rule set.

57. A digital transaction method including:

receiving a first secure container at a user site, the first secure container including first governed content, the first governed content being governed by a first rule set, the first rule set specifying that access to the first governed content requires that the user provide payment and that first usage information relating to the access be collected;

the user indicating an interest in accessing or otherwise using at least some of the first governed content;

a first message being conveyed to the user using an output device, the first message indicating that use of the first governed content requires payment and asking for confirmation that the user desires to make the payment;

the user indicating a desire to make the payment;

under control of the first rule set, first payment information being securely conveyed to a financial clearinghouse and first usage information being securely collected at the user's site:

at the financial clearinghouse, the first payment information being used to provide payment to an owner of rights in the governed content;

receiving a second secure container at the user site, the second secure container including second governed content, the second governed content being governed by a

second rule set, the second rule set specifying that access to the second governed content requires that the user provide payment and that second usage information relating to the access be collected;

the user indicating an interest in accessing or otherwise using at least some of the second governed content;

a second message being conveyed to the user using an output device, the second message indicating that use of the second governed content requires payment and asking for confirmation that the user desires to make the payment;

the user indicating a desire to make the payment;

under control of the second rule set, second payment information being securely conveyed to a financial clearinghouse and second usage information being securely collected at the user's site;

at the financial clearinghouse, the second payment information being used to provide payment to an owner of rights in the governed content; and

at the user's site, the first usage information and the second usage information being analyzed and, based on the results of the analysis, usage information being securely transmitted to an information clearinghouse.

58. A method as in Claim 57, in which the analysis of the first usage information and the second usage information is governed, at least in part, by the first rule set and the second rule set.

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT
& DUNNER, L.L.P.
STANFORD RESEARCH PARK
700 HANSEN WAY
PALO ALTO, CALIF. 94304
650-849-8600

59. A method as in Claim 58, in which the first rule set and the second rule set each contain a rule from the information clearinghouse.

60. A method as in Claim 58, in which the step of securely transmitting usage information to the information clearinghouse includes generating a third secure container, the third secure container having associated a third rule set, the generation of the third secure container being governed, at least in part, by the first rule set and the second rule set.

61. A method as in Claim 60, in which the third rule set includes a rule governing the use which may be made by the information clearinghouse of the transmitted usage information.

62. A digital transaction method including the following:
receiving a first secure container at a user site, the first secure container including governed content, the governed content being governed, at least in part, by a first rule set;
the user indicating an interest in gaining access to at least a portion of the controlled content;
in response to the user's indication, the first rule set causing a set of options to be conveyed to the user, the options including requirements for payment and requirements for the provision of information;

the user selecting an option including a relatively higher price, and relatively greater privacy protections for the information;

in response to the selection, the following actions occurring, at least in part under the control of the first rule set:

the user being provided access to at least a portion of the governed content;

payment and usage information being securely communicated to a first clearinghouse;

the first clearinghouse providing payment information to a second clearinghouse; and

the first clearinghouse removing at least some identifying information from the usage information and providing the altered usage information to the second clearinghouse, the alteration being governed, at least in part, by the privacy protection option selected by the user.

63. A method as in Claim 62, in which the steps which occur in response to the user selection include the creation of a secure container having associated a second rule set, the creation being governed at least in part by the first rule set, the second rule set including one or more rules embodying the privacy protections selected by the user; and

the first clearinghouse removal of identifying information is governed, at least in part, by the second rule set.

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT
& DUNNER, L.L.P.
STANFORD RESEARCH PARK
700 HANSEN WAY
PALO ALTO, CALIF. 94304
650-849-6600

64. A method as in Claim 62, in which the first rule set includes a rule from the first clearinghouse and a rule from an owner of an interest in the governed content.

65. A method as in Claim 64, in which the first rule set includes a rule from the second clearinghouse.

66. A method as in Claim 62, in which the set of options presented to the user includes an option regarding the payment method to be used.

67. A digital transaction method including:
receiving a secure container at a user site, the secure container including governed content, the governed content being governed, at least in part, by a rule set, the rule set containing a rule contributed by a first entity, a rule contributed by a second entity, and a rule contributed by a third entity;
communicating to the user a message including an option relating to access to or other use of the governed content, including terms under which such access or use will be allowed, the terms being consistent with requirements specified by the rule set;
the user choosing to access at least a portion of the governed content, and indicating agreement to the specified terms for access;
in compliance with the agreed-upon terms, the user securely communicating payment information and usage information to the first entity, the communication being controlled, at least in part, by the rule set;

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT
& DUNNER, L.P.
STANFORD RESEARCH PARK
700 HANSEN WAY
PALO ALTO, CALIF. 94304
650-849-6600

the first entity aggregating the payment information together with other payment information and securely communicating the aggregated payment information to the second entity, the communication being at least in part governed by the rule supplied by the second entity;

the first entity analyzing the usage information and using the results of that analysis in the process of preparing a usage report; and

the first entity securely communicating the usage report to the third entity, the communication being at least in part governed by the rule supplied by the third entity.

B
68. A digital transaction method including:

at a user site, securely receiving a first rule from a first entity, the first rule being designed to at least in part govern the collection and transmission of information relating to a digital transaction;

at the user site, the first rule securely interacting with a second rule, the second rule also being designed to at least in part govern the collection and transmission of information relating to a digital transaction;

as a result of the interaction between the first rule and the second rule, creating a first rule set, the first rule set specifying at least one aspect of collection of information relating to a digital transaction, and further specifying at least one recipient of information relating to a digital transaction;

at the user site, the user agreeing to comply with terms required for completion of a digital transaction, the terms being at least in part specified by the first rule set;

at the user site, securely collecting information relating to the digital transaction, the collection being governed at least in part by the first rule set; and
securely transmitting at least a portion of the collected information to the first entity, the transmission being governed at least in part by the first rule set.

69. A digital transaction as in Claim 68, in which:

the second rule includes requirements relating to the manner in which personal information relating to the user will be transmitted to or used by the first entity.

70. A digital transaction as in Claim 68, further including:

at the user site, securely receiving a third rule from a second entity, the third rule being designed to at least in part govern the collection and transmission of information relating to a digital transaction;

at the user site, the third rule interacting with the second rule;

as a result of the interaction between the third rule and the second rule, creating a second rule set, the second rule set specifying at least one aspect of collection of information relating to a digital transaction, and further specifying at least one recipient of information relating to a digital transaction;

at the user site, the user agreeing to comply with terms required for completion of a digital transaction, the terms being at least in part specified by the second rule set;

at the user site, securely collecting information relating to the digital transaction, the collection being governed at least in part by the second rule set; and

securely transmitting at least a portion of the collected information to the second entity, the transmission being governed at least in part by the second rule set.

71. A digital transaction method including:

generating a first rule set including a first rule from a first entity and a second rule from a second entity, the first rule set being designed to at least in part govern the collection of payment and usage information relating to a digital transaction;

securely transmitting the first rule set to a user site;
at the user site, communicating terms for the digital transaction to a user, the terms being governed at least in part by the first rule set

the user indicating agreement with at least some of the communicated terms;
at the user site, the first rule set securely interacting with a third rule to create a second rule set, the second rule set being designed to at least in part govern the collection of payment and usage information relating to the digital transaction;

in compliance with the third rule set, payment information and usage information being securely stored at the user site;

in compliance with the third rule set, the collected payment information and usage information being securely communicated to the first entity;

at the first entity, the payment information and usage information being governed by the third rule set; and

in compliance with the requirements of the third rule set, a subset of the usage information being securely communicated from the first entity to the second entity.

72. A digital transaction method including the following:

- a first entity transmitting a secure container to a user, the secure container including governed content, the governed content being governed, at least in part, by a first rule set, the first rule set including a first rule from the first entity and a second rule from a second entity, the second entity having an interest in at least a portion of the governed content, the second rule specifying a requirement which must be met in order for access to at least a portion of the governed content to be authorized;
- the user indicating an interest in obtaining access to at least a portion of the governed content;
- the first rule set securely interacting with a second rule set present on the user's computer, the second rule set including at least one rule relating to agreement terms which are required or desired by the user;
- the interaction resulting in an indication that the requirements of the first rule set and the requirements of the second rule set are inconsistent;
- as a result of the indication, a secure communication being initiated between the user site and the first entity, the communication including a request for access to at least a portion of the governed content on terms which are inconsistent with the requirements of the second rule;
- the first entity comparing the terms contained in the communication with acceptable terms previously communicated by the second entity and determining that a match exists;

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT
& DUNNER, L.L.P.
STANFORD RESEARCH PARK
700 HANSEN WAY
PALO ALTO, CALIF. 94304
650-849-6600

B1

the first entity generating a third rule set without further communication with the second entity, the third rule set being consistent with the terms proposed in the communication;

the third rule set being securely communicated to the user site;

the third rule set securely interacting with the second rule set, resulting in an indication that agreement has been reached;

the user receiving access to at least a portion of the governed content, the access being governed at least in part by the third rule set;

under control of the third rule set, the user securely providing payment information and usage information to the first entity; and

the first entity securely communicating at least a portion of the payment information to the second entity.

73. A financial and rights information clearing system including:

a first clearinghouse at least in part specializing in administering transactions relating to a first digital content type;

a second clearinghouse at least in part specializing in administering transactions relating to a second digital content type; and

a user site including a first secure container and a second secure container, the first secure container including:

first governed content of the first digital content type;

B1

and having associated a first rule set at least in part governing access to or other use of the first governed content, the first rule set requiring payment of consideration for use of the first governed content and also requiring the provision of usage information, the first rule set further requiring that payment information and usage information be securely communicated to the first clearinghouse;

the second secure container including

second governed content of the second digital content type;

and having associated a second rule set at least in part governing access to or other use of the second governed content, the second rule set requiring payment of consideration for use of the second governed content and also requiring the provision of usage information, the second rule set further requiring that payment information and usage information be securely communicated to the second clearinghouse.

74. A digital transaction method including:

communicating a secure container to a user site, the secure container including governed content, the secure container having associated a rule set at least in part governing access to or other use of the governed content, the rule set specifying at least a first clearinghouse and a second clearinghouse;

the user indicating an interest in obtaining access to at least a portion of the governed content;

in response to the user indication, the rule set communicating to the user information relating to the terms under which access will be granted, the terms including

the requirement that payment information and usage information be communicated to a clearinghouse;

the user indicating agreement with the terms;

the rule set authorizing access to the governed content;

the rule set determining whether a first governmental entity or a second governmental entity has jurisdiction over the digital transaction; and

based on the determination, the rule set causing the payment information and usage information to be securely communicated to the first clearinghouse if the first governmental entity has jurisdiction and to the second clearinghouse if the second governmental entity has jurisdiction.

B

75. A digital transaction method including:

the user selecting a first clearinghouse from a list of clearinghouse options, the selection being stored in the user's computer;

the user receiving a secure container including governed content, the governed content having associated a rule set, the rule set specifying terms and conditions under which access to the governed content will be granted, the terms and conditions including a list of clearinghouses which are authorized;

the user indicating interest in obtaining access to at least a portion of the governed content;

in response to the user indication, the rule set comparing the clearinghouse selection stored in the user's computer to the list of authorized clearinghouses;

if the stored clearinghouse selection is consistent with the list of authorized clearinghouses, the rule set authorizing the transaction, following which the user obtains access to at least a portion of the governed content and payment and usage information is communicated to the first clearinghouse;

if the stored clearinghouse selection is not consistent with the list of authorized clearinghouses, the rule set causing a message to be communicated to the user, the message indicating that the stored clearinghouse selection is not acceptable and providing at least one alternate clearinghouse option;

if the user agrees to the alternate clearinghouse option, the rule set authorizing the transaction, following which the user obtains access to at least a portion of the governed content and payment and usage information is communicated to the alternate clearinghouse; and

if the user does not agree to the alternate clearinghouse option, the rule set causing a message to be communicated to the user, the message indicating that access to the governed content has not been authorized.

76. A method of administering a digital transaction including:

generating a first rule set, the first rule set including a first rule identifying a first data center and a second rule specifying terms for use of digital content, the terms including the provision of usage-related information;

generating a first secure container, the first secure container including governed content;

associating the first rule set with the first secure container;

communicating the first secure container to a user site;

at the user site, a user agreeing to the terms for usage specified by the second rule;

the first rule set authorizing the user to gain access to at least a portion of the governed content;

in compliance with the first rule, usage information relating to the user's access to the governed content being gathered at the user site;

in compliance with the first rule, the gathered usage information being incorporated into a second secure container;

in compliance with the first rule, generating a second rule set, the second rule set including a third rule specifying communication of the second secure container to the first entity, and a fourth rule specifying at least one privacy option chosen by the user;

securely communicating the second secure container to the first entity;

in compliance with the fourth rule, the first entity aggregating the communicated usage information together with usage information relating to other digital transactions and securely communicating the aggregated information to a second entity; and

in compliance with the fourth rule, the first entity altering the communicated usage information so as to remove certain privacy-related information and securely communicating the altered usage information to a fourth entity.

77. A method as in Claim 76, in which:

the step of generating the second rule set includes:

providing the user at least two options regarding the manner in which the first entity may use communicated usage information;
the user selecting one of the provided options; and
the fourth rule incorporating information relating to the option selected by the user.

78. A method as in Claim 77, in which:

the options provided to the user include an option relating to the identity of one or more entities to which the first entity will be authorized to communicate at least some of the usage information.

79. A method as in Claim 78, in which:

the options provided to the user include an option relating to an internal use the first entity will be authorized to make of the communicated usage information.

80. A method as in Claim 79, in which:

the fourth entity owns an interest in at least a portion of the governed content.

81. A digital transaction method including:

at a first electronic data center, receiving a first communication relating to a first digital transaction involving the use of first governed content by a first user, the first communication including first payment information, first usage information and a first rule set made up of at least one rule;

at the first electronic data center, receiving a second communication relating to a second digital transaction involving the use of second governed content by a second user, the second communication including second payment information, second usage information and a second rule set made up of at least one rule;

at the first electronic data center, invoking the first rule set and undertaking the following actions:

determining that the first rule set requires that the first payment information be cleared by the first electronic data center and, in response, determining the amount of payment provided and communicating payment-related information to a rightsholder owning rights in the first governed content, and

determining that the first rule set requires that usage information be analyzed by the first electronic data center, and, in response, performing the analysis and conveying results of the analysis to an external entity without conveying identification information contained in the usage information;

at the first electronic data center, invoking the second rule set and undertaking the following actions:

determining that the second rule set requires that the second payment information be cleared by a second electronic data center and, in response, communicating the payment information and at least one rule from the second rule set to the second electronic data center;

at the second electronic data center, invoking the second rule set rule and undertaking the following actions:

B1

determining that the second rule set rule requires that the second payment information be cleared by the second electronic data center and, in response, determining the amount of payment provided and communicating payment-related information to a rightsholder owning rights in the second governed content, and determining that the second rule set requires that usage information be analyzed by a third electronic data center, and, in response, communicating the usage information and at least one rule from the second rule set to the third electronic data center,

the third electronic data center determining that the second rule set rule requires that usage information be analyzed by the third electronic data center, and, in response, performing the analysis and conveying results of the analysis to an external entity without conveying identification information contained in the usage information.

82. A method as in Claim 81, further including:

at a site associated with the first user, receiving a first secure container containing the first governed content and generating the first rule set, the first rule set including information provided by the first electronic data center and information provided by the first user; and

at a site associated with the second user, receiving a second secure container containing the second governed content and generating the second rule set, the second rule set including information provided by the second electronic data center and information provided by the second user.

83.

A method as in Claim 82, in which:

the step of generating the first rule set includes the first user choosing the first data center for clearance of payment information, and choosing the first data center for analysis of usage information; and

the step of generating the second rule set includes the second user choosing the second data center for clearance of payment information, and choosing the third data center for analysis of usage information.

84.

A method as in Claim 81, further including:

at the first electronic data center, receiving a third communication relating to a third digital transaction involving the use of third governed content by a third user, the third communication including third payment information, third usage information and a third rule set made up of at least one rule;

at the first electronic data center, invoking the third rule set and undertaking the following actions:

determining that the third rule set requires that the third payment information be cleared by the first electronic data center and, in response, determining the amount of payment provided and communicating payment-related information to a rightsholder owning rights in the third governed content, and

determining that the third rule set requires that usage information be analyzed by a fourth electronic data center, and, in response, communicating the usage information and at least one rule from the third rule set to the fourth electronic data center,

the fourth electronic data center determining that the third rule set rule requires that usage information be analyzed by the fourth electronic data center, and, in response, performing the analysis and conveying results of the analysis to an external entity without conveying identification information contained in the usage information.

85. A method as in Claim 84, in which the external entity consists of the first electronic data center.

86. A method of administering a digital transaction including the following:

receiving a first secure container at a user site, the first secure container including first governed content and having associated a first rule set;

at the user site, gaining access to at least a portion of the first governed content, the access being governed, at least in part, by the first rule set;

in compliance with the first rule set, securely communicating first payment information and first usage information relating to the first governed content access to an electronic data center, the communication occurring substantially contemporaneously with the access;

at the electronic data center, analyzing the first usage information and communicating at least some results of the analysis to another electronic data center;

receiving a second secure container at the user site, the second secure container including second governed content and having associated a second rule set;

at the user site, gaining access to at least a portion of the second governed content, the access being governed, at least in part, by the second rule set;

in compliance with the second rule set, storing second payment information and second usage information relating to the second governed content access, the storage occurring in a secure storage location at the user site;

aggregating the second payment information together with other payment information and securely communicating the aggregated payment information to an electronic data center, the communication occurring non-substantially contemporaneously with the access; and

in compliance with the second rule set, securely analyzing the second usage information at the user site and securely communicating the results of the analysis to an electronic data center.

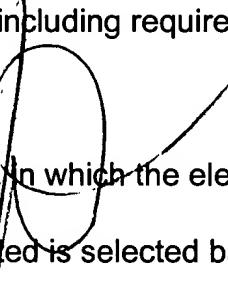
B1

87. A method as in Claim 86, further including:

receiving a third secure container at the user site, the third secure container including third governed content and having associated a third rule set;

in compliance with the third rule set, storing third payment information and third usage information relating to the third governed content access, the storage occurring in a secure storage location at the user site; and

the step of aggregating the second payment information includes aggregating the second payment information with the third payment information.

B 

88. A method as in Claim 87, further including:
in compliance with the third rule set, securely communicating the third usage information to an electronic data center.

89. A method as in Claim 86, further including:
at the user site, comparing the requirements of the first rule set to the requirements of a third rule set, the third rule set including requirements specified by the user.

90. A method as in Claim 89, in which the electronic data center to which the first payment information is communicated is selected based at least in part on the results of the comparison.

91. A method of administering digital transactions including:
at a user site, generating payment information and usage information relating to a digital transaction;
securely communicating the generated information to an electronic data center;
at the electronic data center, communicating the payment information to a financial clearinghouse;
at the electronic data center, analyzing the usage information to identify an attribute of the user or user site;
selecting an information clearinghouse from at least two information clearinghouses, the selection being at least in part based on the identified attribute;

communicating the usage information from the electronic data center to the selected information clearinghouse; and

the selected information clearinghouse analyzing the usage information, generating a report, and communicating the report to a third party.

92. A method as in Claim 91, in which:

the step of selecting an information clearinghouse further includes matching the identified user attribute to an attribute of the selected clearinghouse and basing the selection at least in part on the match.

93. A method as in Claim 92 further including:

securely communicating a rule set comprising at least one rule from the user site to the electronic data center;

and in which the step of selecting an information clearinghouse is governed at least in part by the rule set.

94. A method as in Claim 92 in which the step of analyzing the usage information further includes aggregating the usage information together with other usage information and the third party constitutes an owner of a right associated with the subject of the digital transaction.

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT
& DUNNER, L.L.P.
STANFORD RESEARCH PARK
700 HANSEN WAY
PALO ALTO, CALIF. 94304
650-849-8600

95. A method as in Claim 94, further including:
communicating a rule set from the right owner to the information clearinghouse;
and in which the step of analyzing the usage information is governed at least in part
by the rule set.

96. A first digital clearinghouse node including:
storage means for storing:
a first rule set,
the first rule set including a rule from a first user of governed content and a rule
from the first digital clearinghouse,
the first rule set specifying that:
the first digital clearinghouse perform a first step in clearing a transaction
involving the first user's use of governed content, and
a different digital clearinghouse perform a second step in clearing the
transaction involving the first user's use of governed content; and
a second rule set,
the second rule set including a rule from a second user of governed content
and a rule from the first digital clearinghouse,
the second rule set specifying that:
the first digital clearinghouse perform the second step in clearing a
transaction involving the second user's use of governed content, and

a different digital clearinghouse perform the first step in clearing the transaction involving the first user's use of governed content.

97. A first digital clearinghouse as in Claim 96, in which the first rule set includes a rule from the different clearinghouse specified for performing the second step in clearing the first transaction.

98. A first digital clearinghouse as in Claim 96, in which the first step involves aggregating financial information and communicating at least a portion of the aggregated financial information to a rightsholder.

99. A first digital clearinghouse as in Claim 97, in which the second step involves aggregating usage information and communicating at least a portion of the aggregated usage information to a third party.

100. A first digital clearinghouse as in Claim 96, in which the first rule set includes a rule at least in part specifying the different clearinghouse use for performing the second step in clearing the transaction involving the first user's use of governed content.

101. A method for receiving value in response to an electronic event, said method comprising:

B 1

- a. Establishing a distributed computing environment supporting peer-to-peer, securely interoperable participant nodes;
- b. Specifying requirements that are securely associated with digital events for at least in part managing the processing of said events at least in part within protected processing environments located at said participant nodes;
- c. Processing a digital event at least in part within a protected processing environment at a first participant's node at least in part in response to an event request authorized by said first participant;
- d. Requiring compensation from said first participant based, at least in part, on the processing of said digital event at said first participant's node; and
- e. Requiring compensation from a second environment participant based, at least in part, on providing usage information related to said digital event.

102. A method as in Claim 101 further including the step of implementing said peer-to-peer, securely interoperable participant nodes with protected processing environments that employ secure processing units and/or tamper-resistant software environments.

103. A method as in Claim 101 further including the step of implementing said peer-to-peer, securely interoperable participant nodes using secure databases.

104. A method as in Claim 101 in which said processed digital event includes a secure negotiation process.

105. A method as in Claim 101 in which said digital event processing involves use of digital information and further including the following steps:
receiving said digital information at said first participant's node,
receiving at least one digital control at said first participant's node, said digital control being received separately from said digital information, and
using said digital control to govern at least one aspect of said digital event.

106. A method as in Claim 101 further including the step of allowing a value chain participant to stipulate at least one aspect of information privacy control.

107. A method for reporting electronic commerce event, user profiling, and/or surveying information, said method comprising the steps of:

- Monitoring usage of digital information at distributed electronic commerce nodes;
- Securely communicating information related to said monitored usage from at least one of said commerce nodes to a first commerce utility system serve;
- In accordance with rules and controls, a first portion of said reported usage related information being provided to said first system serve in a form rendering said portion unusable at said first system service;

BD
LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT
& DUNNER, L.L.P.
STANFORD RESEARCH PARK
700 HANSEN WAY
PALO ALTO, CALIF. 94304
650-849-6600

B1

- d. In accordance with rules and controls related to said communicated usage related information, electronically communicating at least a portion of said first portion to a digital information rightholder; and
- e. at said digital information rightholder, using at least a portion of said electronically communicated information.

108. A method as in Claim 107 further including a value chain participant choosing said first commerce utility system from a group of at least two commerce utility systems.

109. A method as in Claim 107 further including the step of implementing said distributed electronic commerce nodes using secure databases.

110. A method as in Claim 107 further including the step of implementing said commerce utility systems with protected processing environments that employ secure processing units and/or tamper-resistant software environments.

111. A method as in Claim 107 further including the step of implementing said commerce utility systems using secure databases.

112. A method as in Claim 107 in which said usage includes performing a negotiation process.

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT
& DUNNER, L.L.P.
STANFORD RESEARCH PARK
700 HANSEN WAY
PALO ALTO, CALIF. 94304
650-849-6600

113. A method as in Claim 107 in which said usage is governed, at least in part, by at least one digital control, and further including the step of receiving said digital control, said digital control being received separately from said digital information.

114. A method as in Claim 107 further including the step of allowing a value chain participant to stipulate at least one aspect of information privacy control.

115. A distributed computing system supporting peer-to-peer, securely interoperable participant nodes including protected processing environments located at said participant nodes, said system ensuring that value is received in response to an electronic event, said system comprising:

means for enabling the specification of requirements that may be securely associated with discrete digital events for at least in part managing the processing of said events at least in part within said protected processing environments located at said participant nodes;

means for processing a digital event at least in part within a protected processing environment at a first participant's node at least in part in response to an event request authorized by said first participant;

means for requiring compensation from said first participant based, at least in part, on the processing of said digital event at said first participant's node; and

means for requiring compensation from a second system participant based, at least in part, on providing usage information related to said digital event.